Walking the Wire: Network Threat Analysis

Peter Smith and Daniel Beck
MANDIANT

Outline

- Posturing your assets

Outline

- Posturing your assets
- Detection mechanisms and tools

Outline

- Posturing your assets
- Detection mechanisms and tools
- Performing advanced analysis

Outline

- Posturing your assets
- Detection mechanisms and tools
- Performing advanced analysis
- Scoping a compromise

Outline

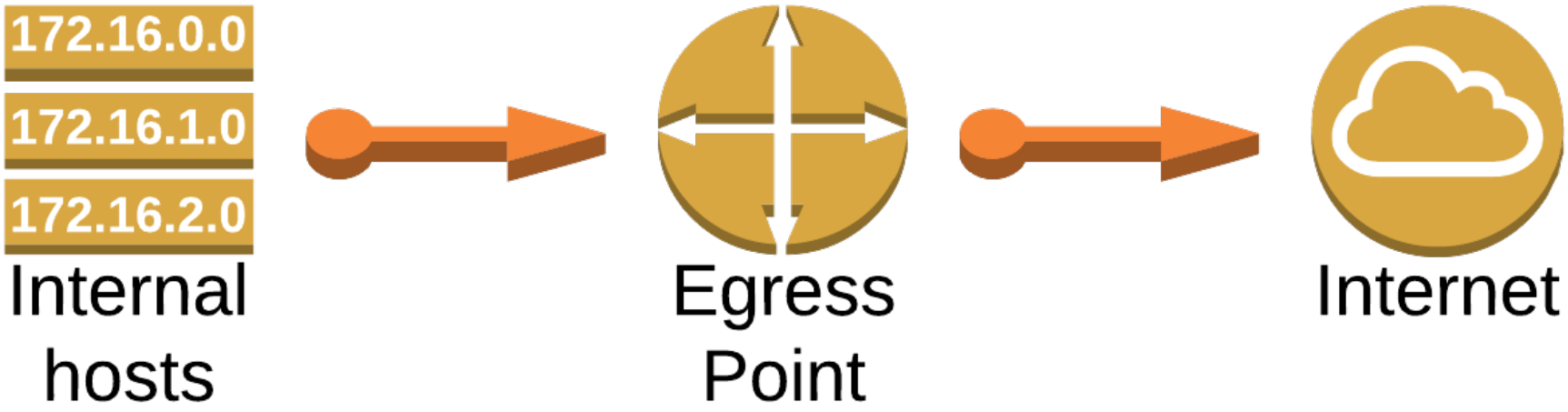
- Posturing your assets
- Detection mechanisms and tools
- Performing advanced analysis
- Scoping a compromise

ALL THINGS DETECTION

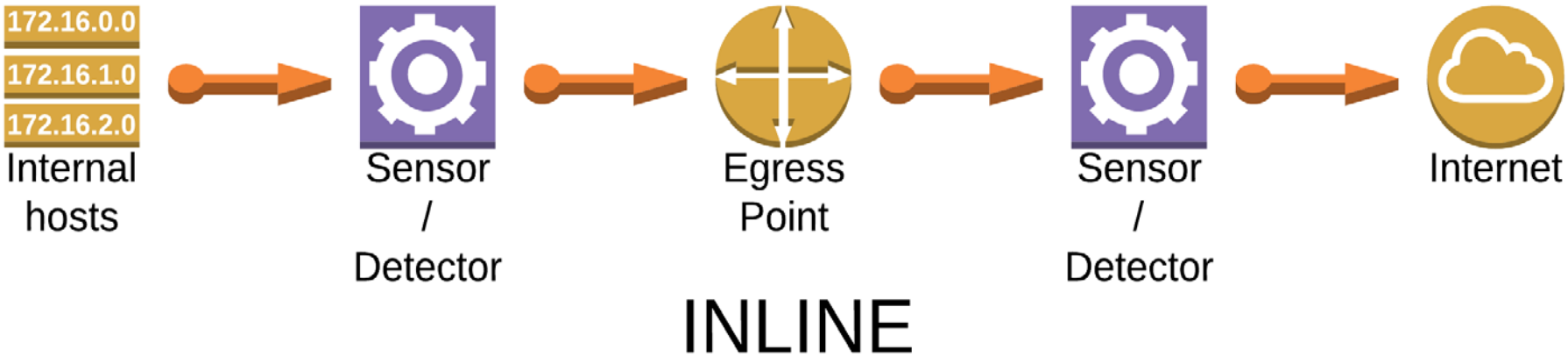
Put your organization in the best possible position to find evil

Detection Platform Positioning

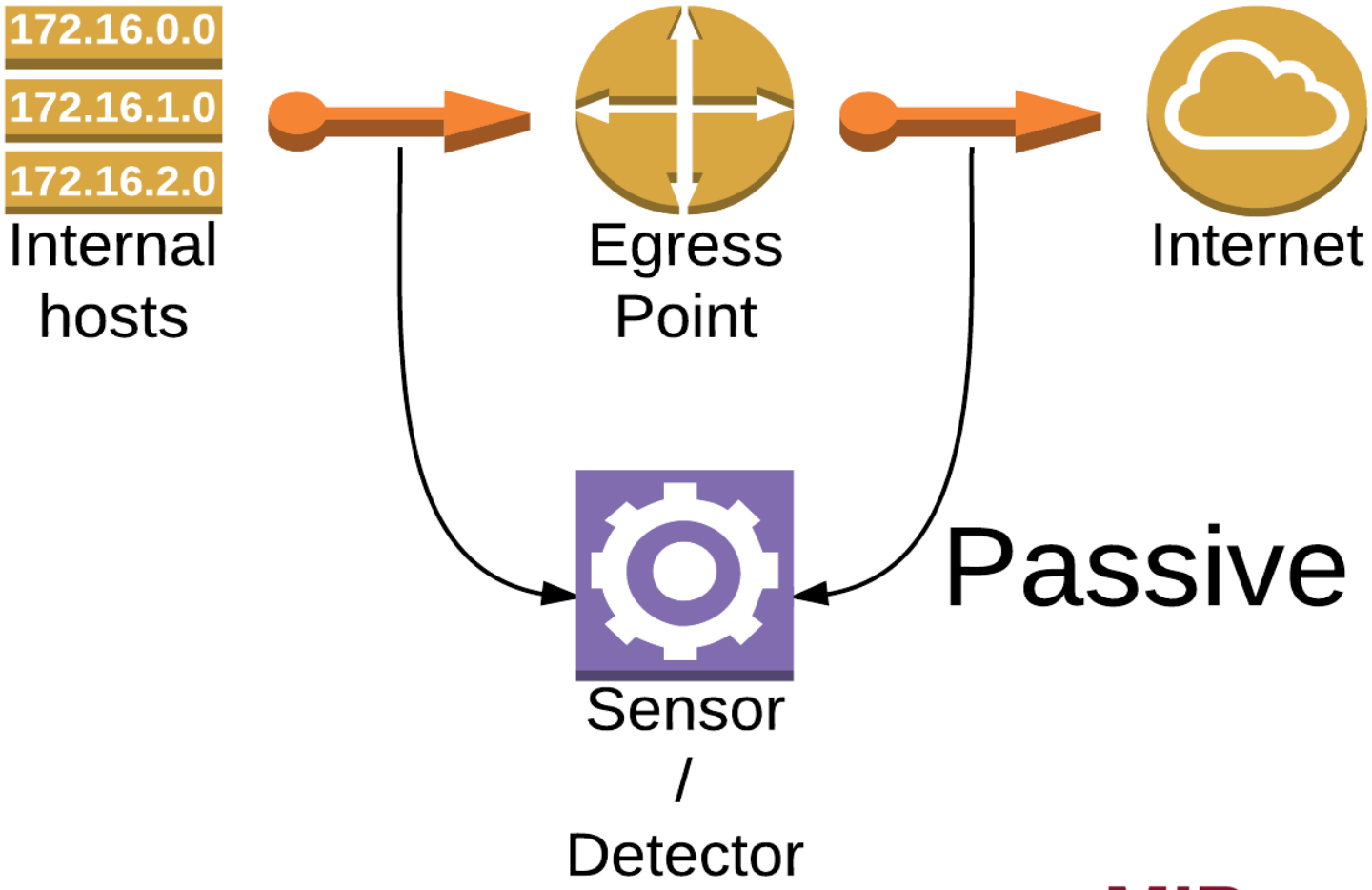
- Inline vs Passive



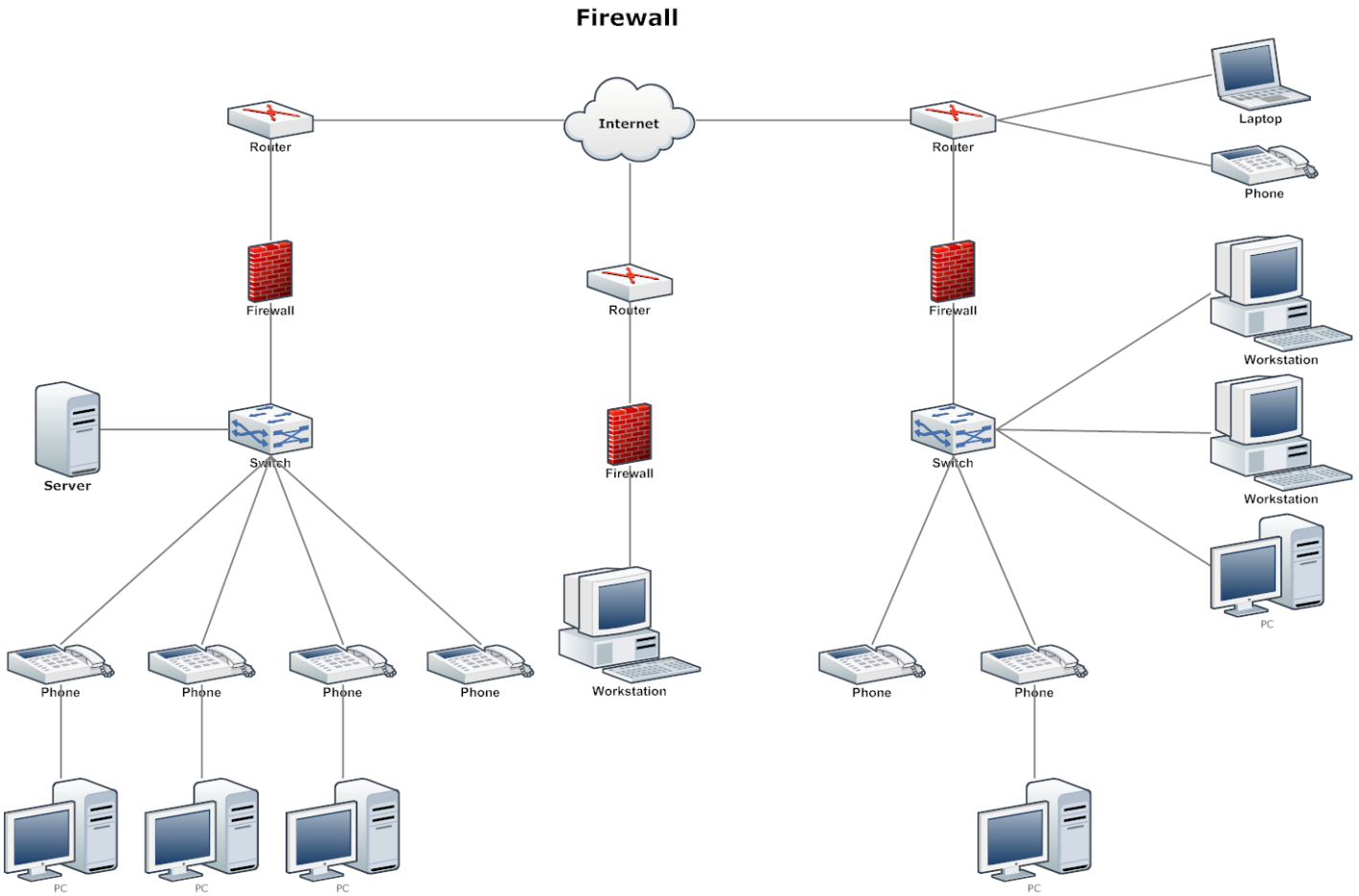
Detection Platform Positioning



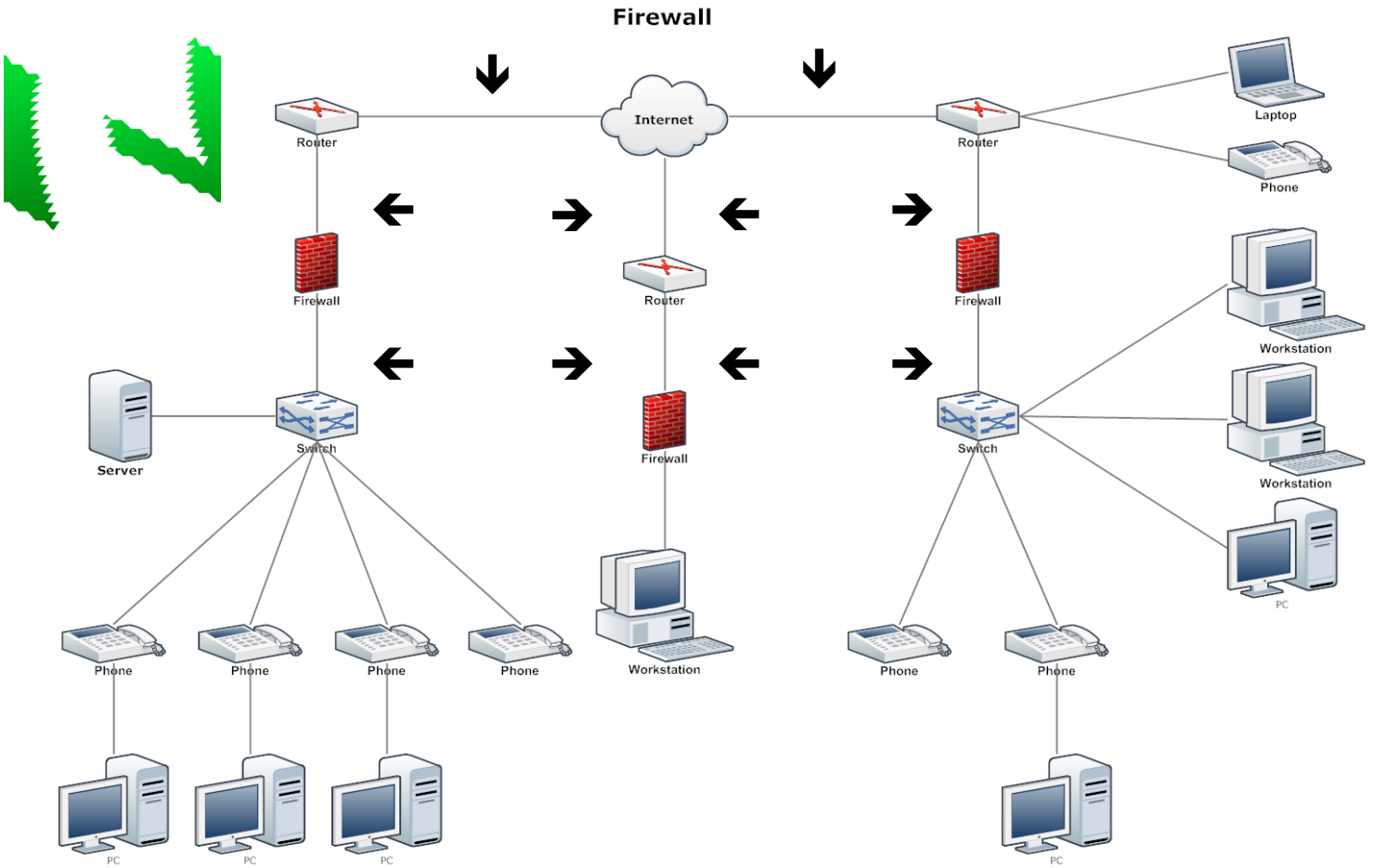
Detection Platform Positioning



Positioning in a Real Network



Positioning in a Real Network



Detection Platform Positioning

- Inline vs Passive
- Capture Data

Detection Platform Positioning

- Inline vs Passive
- Capture Data

Images courtesy http://blog.hostgator.com/2013/04/30/whats-in-a-name-choosing-the-right-domain-name-for-your-website/, http://en.wikipedia.com,

Detection Platform Positioning

- Inline vs Passive
- Capture Data

Images courtesy http://blog.hostgator.com/2013/04/30/whats-in-a-name-choosing-the-right-domain-name-for-your-website/, http://en.wikipedia.com,

Detection Platform Positioning

- Inline vs Passive
- Capture Data

Images courtesy http://blog.hostgator.com/2013/04/30/whats-in-a-name-choosing-the-right-domain-name-for-your-website/, http://en.wikipedia.com,

Detection Platform Positioning

- Inline vs Passive
- Capture Data

Images courtesy http://blog.hostgator.com/2013/04/30/whats-in-a-name-choosing-the-right-domain-name-for-your-website/, http://en.wikipedia.com,

Detection Platform Positioning

- Inline vs Passive
- Capture Data

Images courtesy http://blog.hostgator.com/2013/04/30/whats-in-a-name-choosing-the-right-domain-name-for-your-website/, http://en.wikipedia.com,

Detection Platform Positioning

- Inline vs Passive
- Capture Data

Images courtesy http://blog.hostgator.com/2013/04/30/whats-in-a-name-choosing-the-right-domain-name-for-your-website/, http://en.wikipedia.com,

Detection Technology

Detection Technology

Detection Technology

Detection Technology

Detection Technology

Detection Technology

Detection Technology

Detection Technology

MIRcon 2013

Detection Technology

BlueCoat

IRONPORT SYSTEMS

FireEye™

RSA® NETWITNESS

/* YARA */

SURICATA

MIRcon 2013

Detection Technology

BlueCoat

IRONPORT SYSTEMS

Eye™

RSA® NE

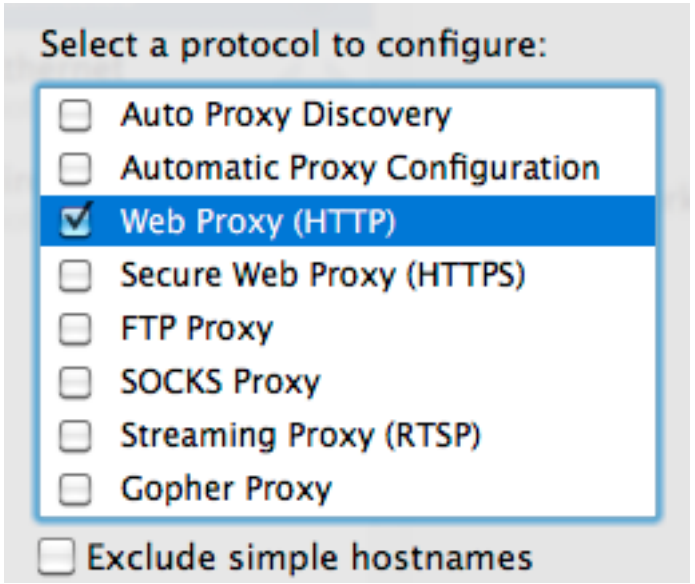
MIRcon 2013

ADVANCED ANALYTICS

Doing more with your data

Advanced Analysis – What We'll Cover

- Web/proxy log analysis



Advanced Analysis – What We'll Cover

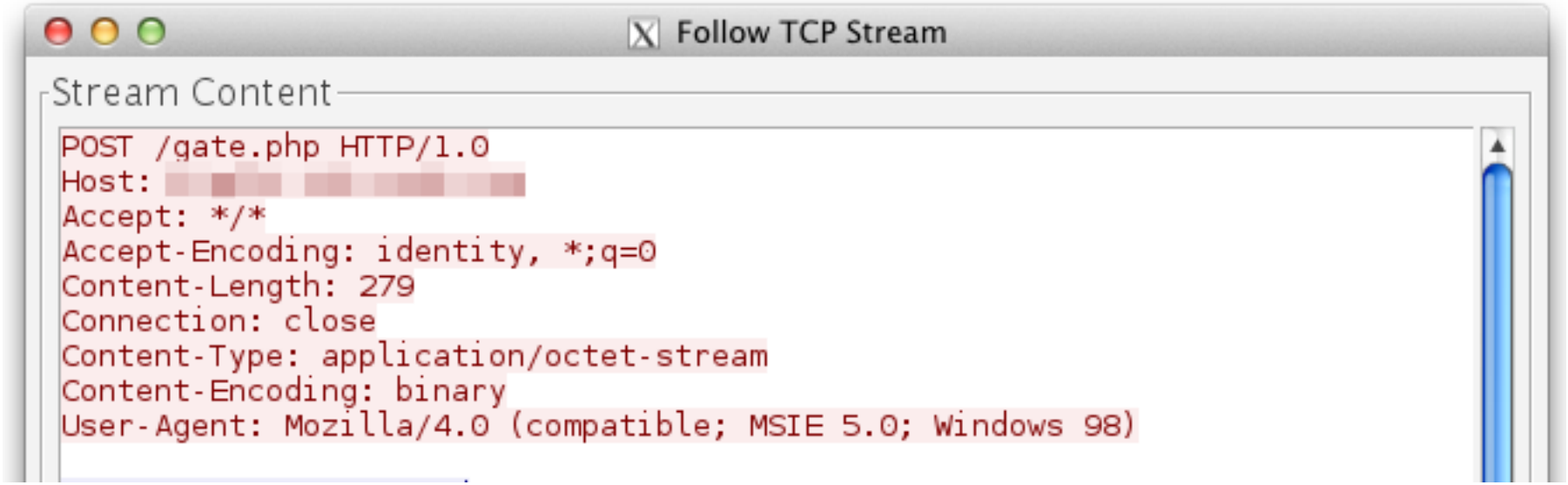
- Web/proxy log analysis
- Baseline and Anomaly Detection

Advanced Analysis – What We'll Cover

- Web/proxy log analysis
- Baseline and Anomaly Detection
- Netflow Analysis

Web/proxy log analysis

- Zeus example
  - GET /config.bin HTTP/1.1 x 1
  - POST /gate.php HTTP/1.1 x 100



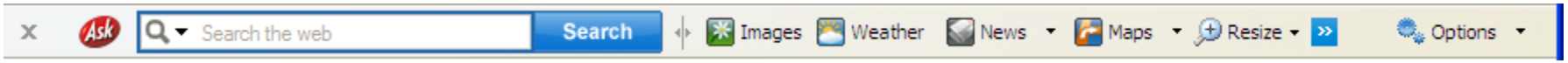
Web/proxy log analysis

- Malware characteristics
  - High ratio of POST/GET requests
  - One or two HTTP paths
  - Single User-Agent to a remote domain


```
"ts" : "29/Oct/2013:14:02:51 +0000", "sa" : "2146965676", "da" : "1741457762", "sp" : "56820", "dp" : "80", "m"  : "GET", "u"
: "/forecastrss", "p"  : "HTTP/1.1", "q" : "p=22314", "ua" : "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8) Gecko/20051111
Firefox/1.5", "rf" : "-", "ho" : "weather.yahooapis.com"
"ts" : "29/Oct/2013:14:02:51 +0000", "sa" : "1845631148", "da" : "1130368080", "sp" : "51588", "dp" : "80", "m"  : "GET", "u"
: "/z/tvecnn_1@135347/tiny_9af6d220098e36e9-p.bootstrap", "p"  : "HTTP/1.1", "q" : "g=OTFSHSDNERIL&hdcore=3.1.0&plugin=aasp-3.1
.0.43.124", "ua" : "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:24.0) Gecko/20100101 Firefox/24.0", "rf" : "http://z.cdn.turner.
com/xslo/cvp/assets/container/2.0.4.0/cvp_main_container.swf", "ho" : "turnerhd-f.akamaihd.net"
"ts" : "29/Oct/2013:14:02:51 +0000", "sa" : "2146965676", "da" : "1741457762", "sp" : "56820", "dp" : "80", "m"  : "GET", "u"
: "/forecastrss", "p"  : "HTTP/1.1", "q" : "p=22314", "ua" : "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.8) Gecko/20051111
Firefox/1.5", "rf" : "-", "ho" : "weather.yahooapis.com"
```

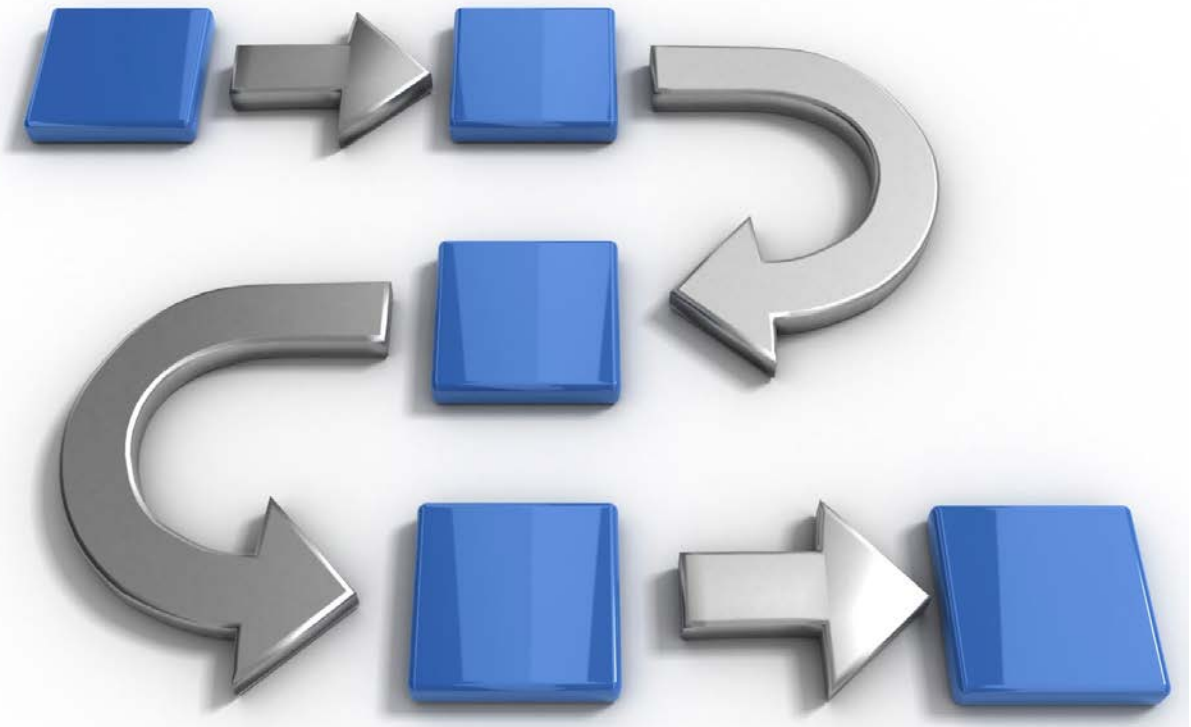
Web/proxy log analysis

- False Positives
  - Web-based live chat
  - Real-time Streaming Protocol
  - Toolbars
  - APIs



Baseline and Anomaly Detection

- Useful for ‘methodology’ activity



Baseline and Anomaly Detection

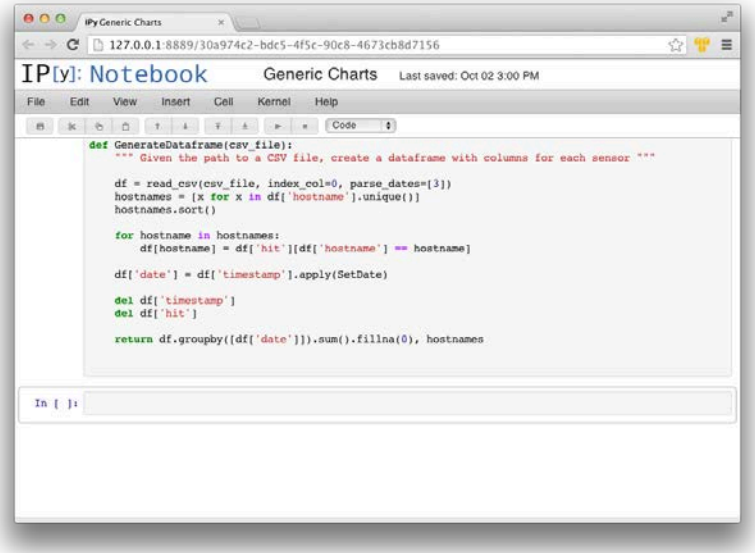
- Useful for ‘methodology’ activity
- Compare present activity to history (duh)

Baseline and Anomaly Detection

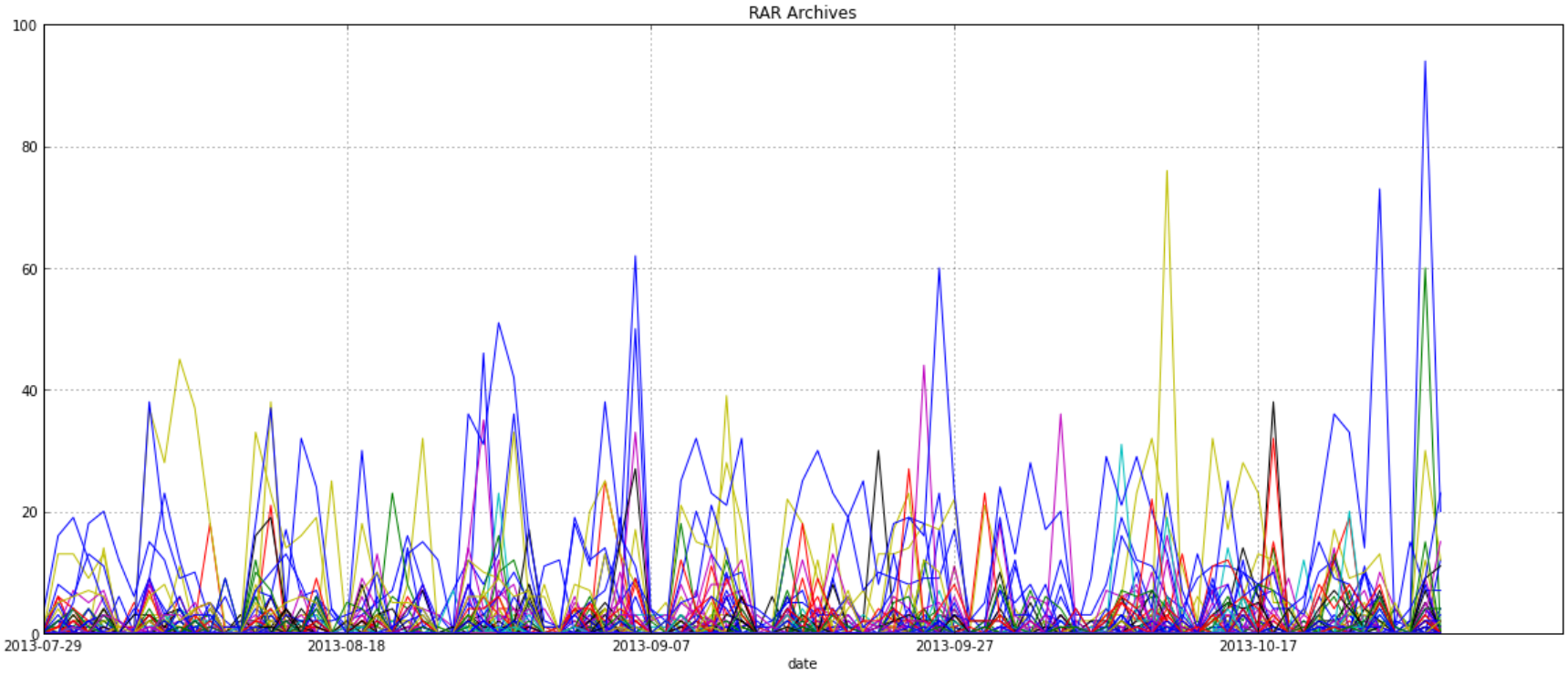
- Useful for ‘methodology’ activity
- Compare present activity to history (duh)
- But how?

Baseline and Anomaly Detection

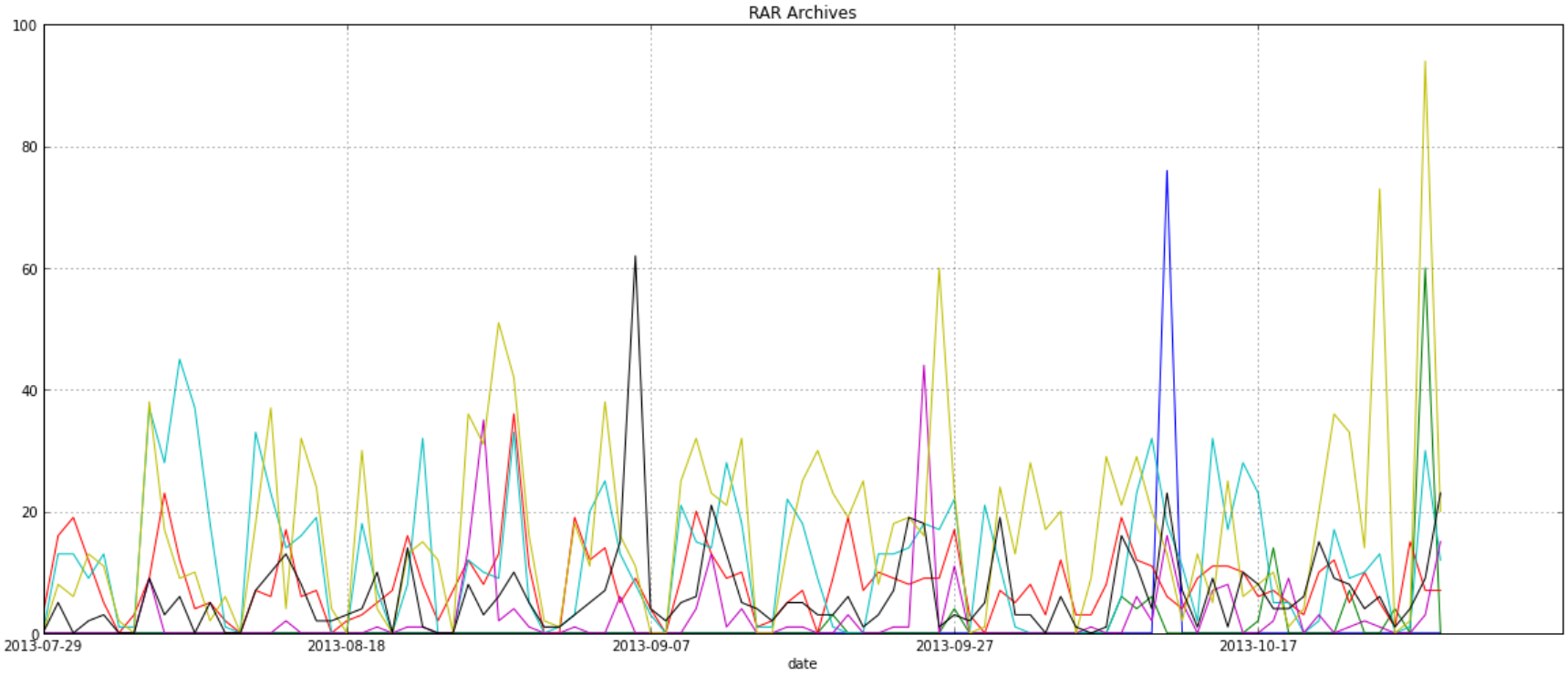
- Tools
  - iPython Notebook
  - Pandas
  - Matplotlib
- Math
  - Standard deviations
  - Rolling averages
  - Quantiles


IPy Generic Charts
127.0.0.1:8889/30a974c2-bdc5-4f5c-90c8-4673cb8d7156
IP[y]: Notebook
Generic Charts
Last saved: Oct 02 3:00 PM
File Edit View Insert Cell Kernel Help
Code
def GenerateDataframe(csv_file):
""" Given the path to a CSV file, create a dataframe with columns for each sensor """
df = read_csv(csv_file, index_col=0, parse_dates=[3])
hostnames = [x for x in df['hostname'].unique()]
hostnames.sort()
for hostname in hostnames:
df[hostname] = df['hit'][df['hostname'] == hostname]
df['date'] = df['timestamp'].apply(SetDate)
del df['timestamp']
del df['hit']
return df.groupby([df['date']]).sum().fillna(0), hostnames
In [ ]:

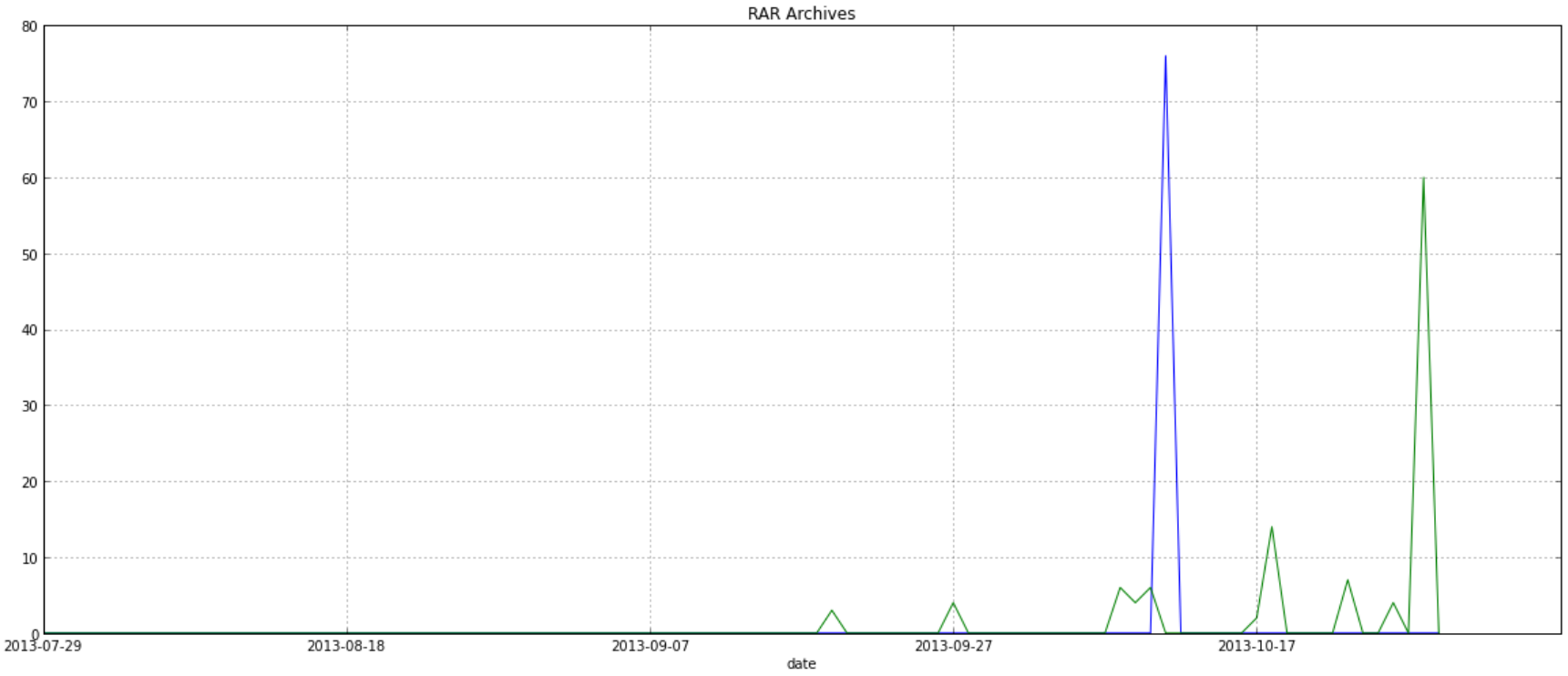
Baseline and Anomaly Detection



Baseline and Anomaly Detection



Baseline and Anomaly Detection

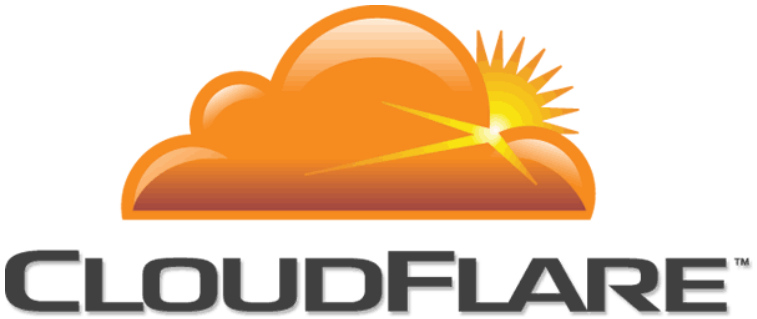


Netflow Analysis

- Apply baselining principles

Netflow Analysis

- Apply baselining principles
- Some caveats
  - Content Delivery Networks



Netflow Analysis

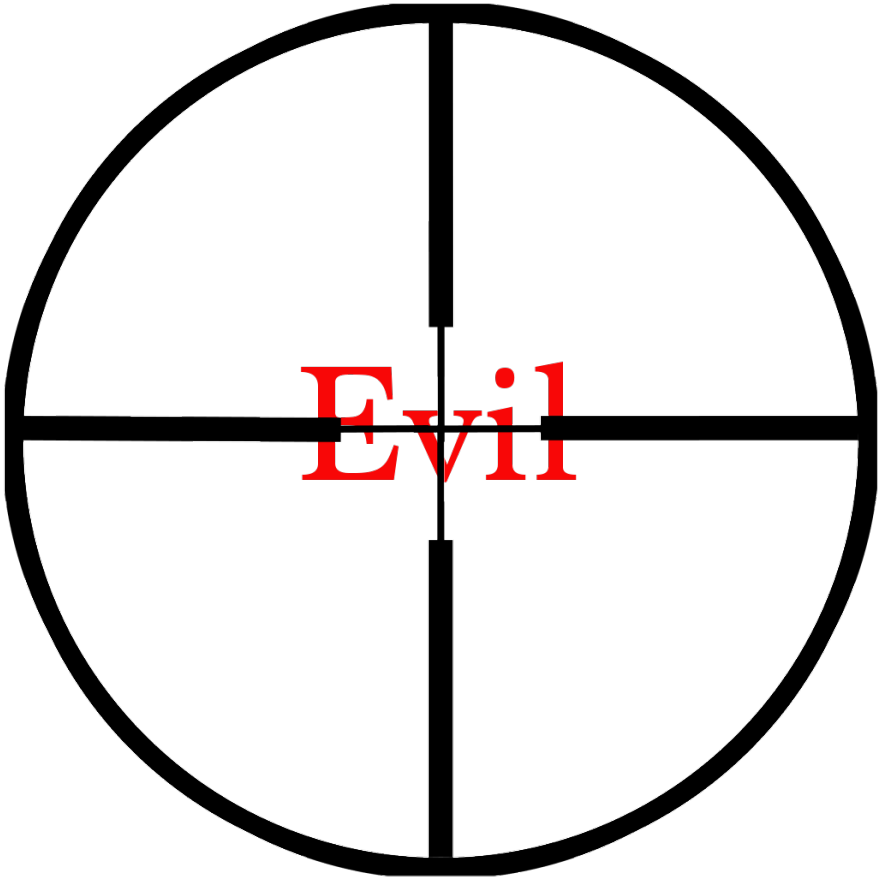
- Apply baselining principles
- Some caveats
  - Content Delivery Networks
  - File storage/backup services

Netflow Analysis

- Apply baselining principles
- Some caveats
  - Content Delivery Networks
  - File storage/backup services
  - Need a good baseline

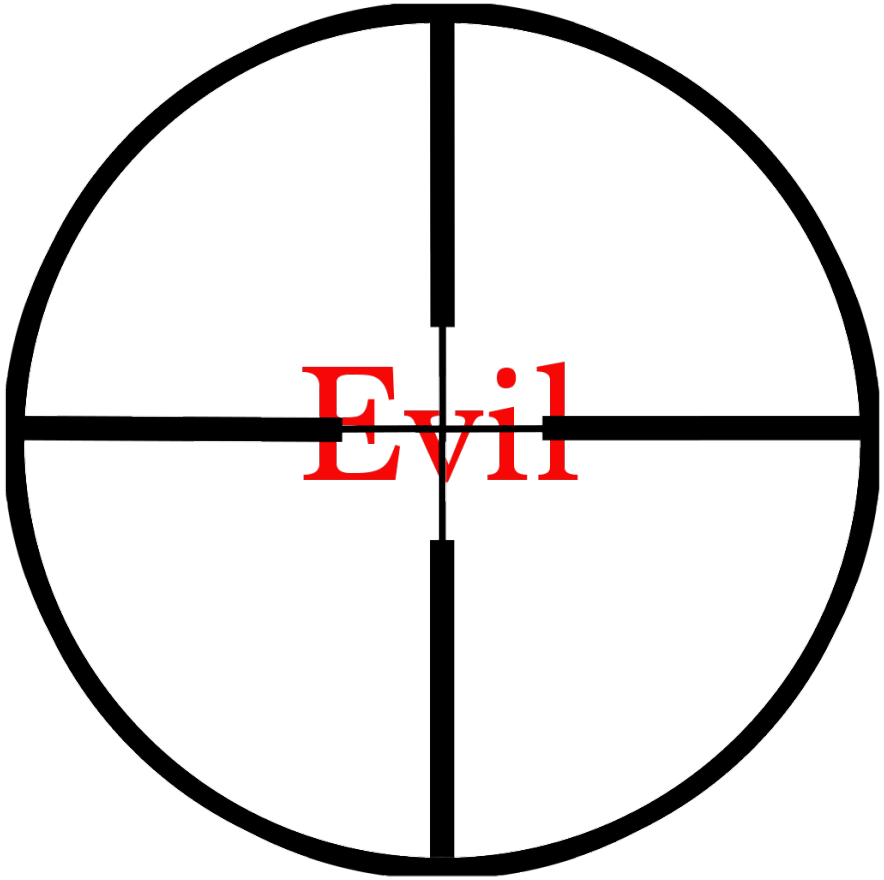
SCOPING A COMPROMISE

Scoping a Compromise



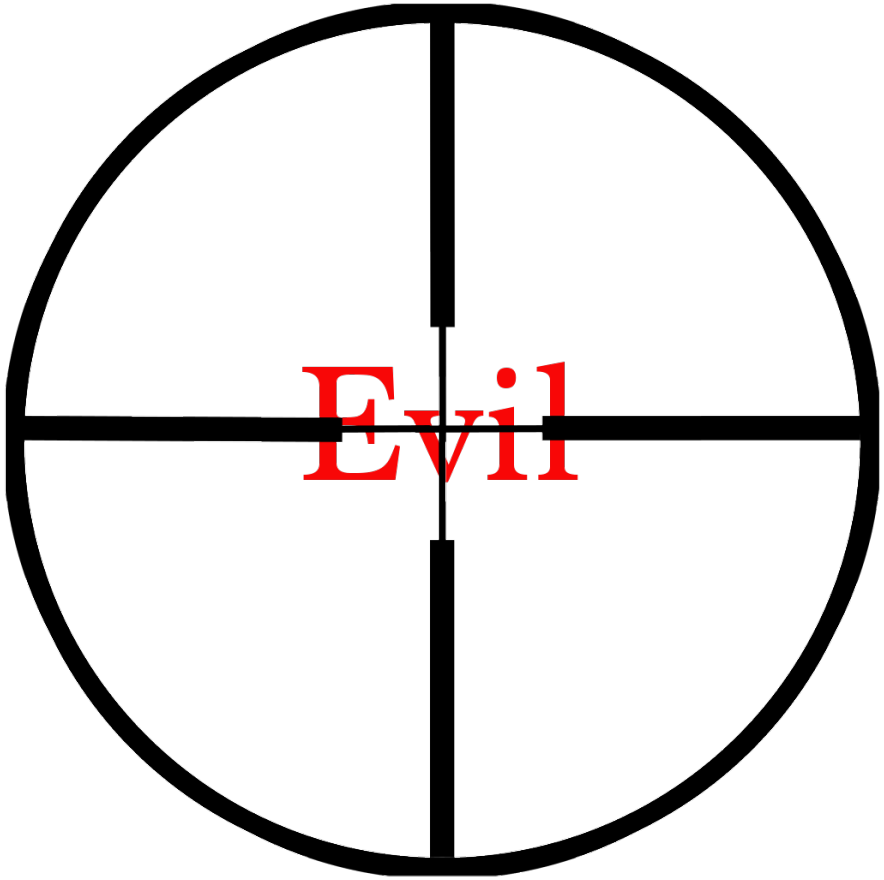
Scoping a Compromise

- It doesn't end at initial detection



Scoping a Compromise

- It doesn't end at initial detection
- Consider your data sources and context

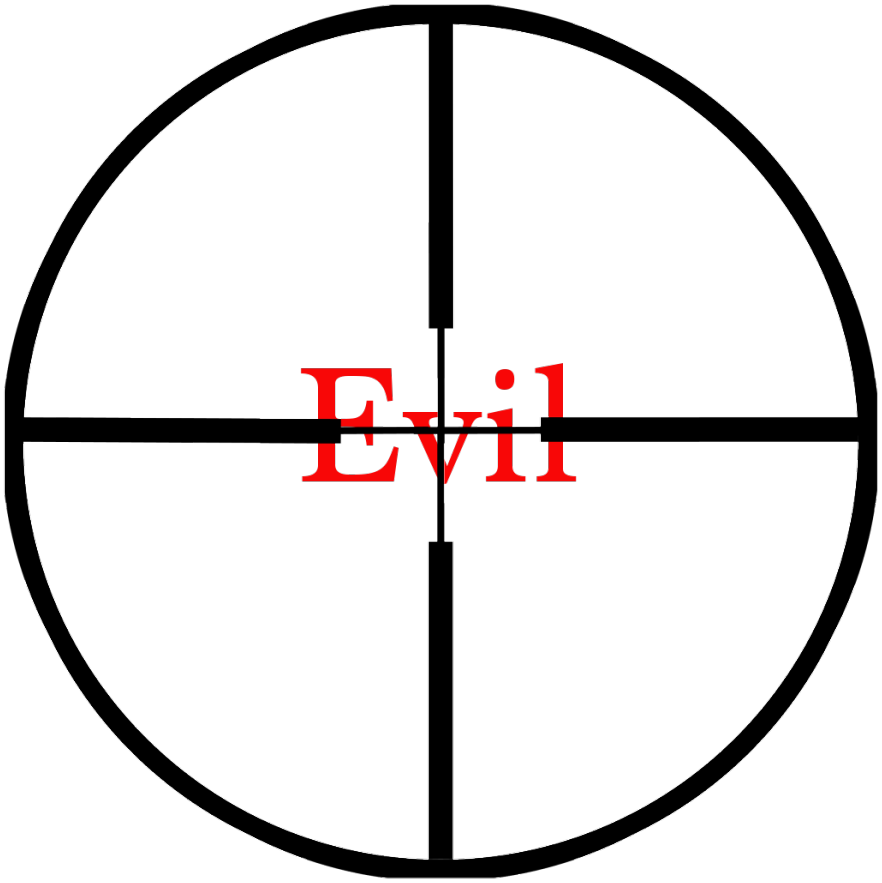


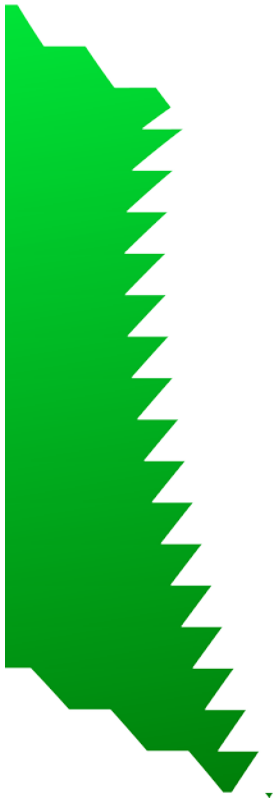
Scoping a Compromise

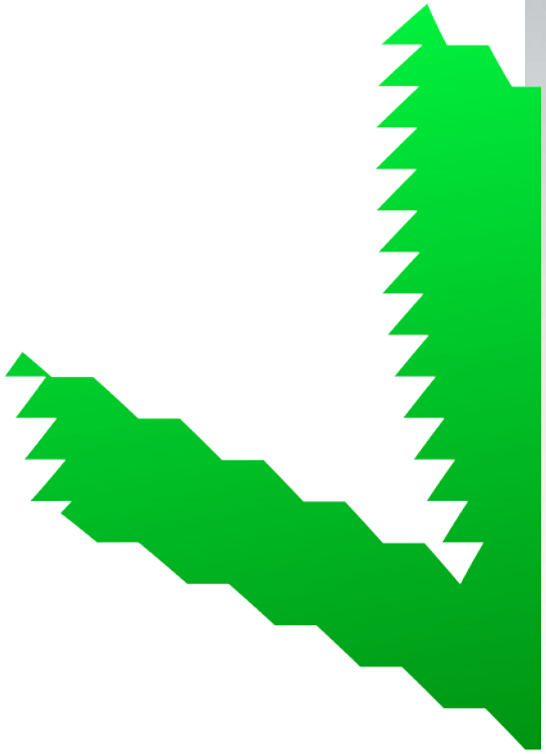
- It doesn't end at initial detection
- Consider your data sources and context
- The iterative approach

Remediate!

- Have you scoped the compromise?







QUESTIONS?

Peter.Smith@mandiant.com
Daniel.Beck@mandiant.com